UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/733,057	12/11/2000	Wataru Inoha	0102/0150	2767

21395 7590 07/01/2004

LOUIS WOO
LAW OFFICE OF LOUIS WOO
717 NORTH FAYETTE STREET
ALEXANDRIA, VA 22314

EXAMINER	
NALVEN, ANDREW L	
ART UNIT	**PAPER NUMBER**
2134	6

DATE MAILED: 07/01/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/733,057	INOHA ET AL.
	Examiner	Art Unit
	Andrew L Nalven	2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 December 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 August 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *2,4*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-16 are pending.

2. Information disclosure statements submitted 3-16-2001 and 8-15-2002 have been received and considered.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Miyano US Patent No. 5,442,705 in view of Bruce Schneier's Applied Cryptography. Miyano discloses a hardware arrangement for enciphering bit blocks while renewing a key at each iteration.

5. With regards to claims 1-2, 9-10, Miyano discloses the rearranging of bits of a first bit sequence in a first matrix according to a predetermined arrangement rule where the sequence representing the information is the base of a key (Miyano, column 2 line 65 – column 3 line 1), the forming of blocks in the first matrix wherein each of the blocks has bits and the number of bits is smaller than the number of bits composing the first matrix (Miyano, column 3 lines 15-19), executing logical operations among bits in each of the blocks and generating a bit being a result of the logical operation (Miyano, column

3 lines 30-34), combining the logical operation bits into a second bit sequence wherein the number of bits composing the second bit sequence is smaller than the number of bits composing the first bit sequence (Miyano, column 3 lines 30-49). Miyano fails to disclose a second matrix composed of a predetermined bit sequence and reading out from among the third bit sequences. Schneier discloses the accessing of a second matrix composed of predetermined third bit sequences and reading out one from among the third bit sequences in response to the second bit sequence and outputting the read out third bit sequence as information representative of the key wherein the number of bits composing each of the third bit sequences is smaller than the number of bits composing the second bit sequence (Schneier, pages 274-275 "The S-Box Substitution", Figure 12.4). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Schneier's method of accessing a second matrix with Miyano's scheme of key renewal because it offers the advantage of making it more difficult to cryptanalyze the key generation procedure because the method is nonlinear.

6. With regards to claims 3-6, 11-14, Miyano teaches all that is described above, and further teaches the encrypting and decrypting of contents of information in response to the key signal (Miyano, Figure 1, column 2 lines 47-55, column 1 lines 17-31).

7. With regards to claims 7 and 15, Miyano as modified teaches the storing of encryption resultant key base information and encryption result contents information (Miyano, column 3 lines 46-49, Abstract).

8. With regards to claims 9 and 16, Miyano as modified teaches the transmitting of encryption result key base information and encryption result contents information through a transmission line (Miyano, column 1 lines 16-24).

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

10. Aiello et al US Patent No. 5,892,829 discloses a method and apparatus for generating a secure hash function.

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew L Nalven whose telephone number is 703 305 8407. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on 703 308 4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Nalven

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100